CryptoMove

Security Direction Report

Overview

This purpose of this report is to provide advice and direction toward reducing the attack surface and improving the security in accordance to the Open Source Security Testing Methodology Manual v3 (OSSTMM). The tests were made using standard security and networking tools. Vulnerability tests were made using Netsense Gravity (https://gravity.netsense.ch) and exploit research from Picus (https://www.picussecurity.com). Initial scope began with the following information:

IPv4 Addresses: [redacted]

Domains: [redacted]

Security Overview

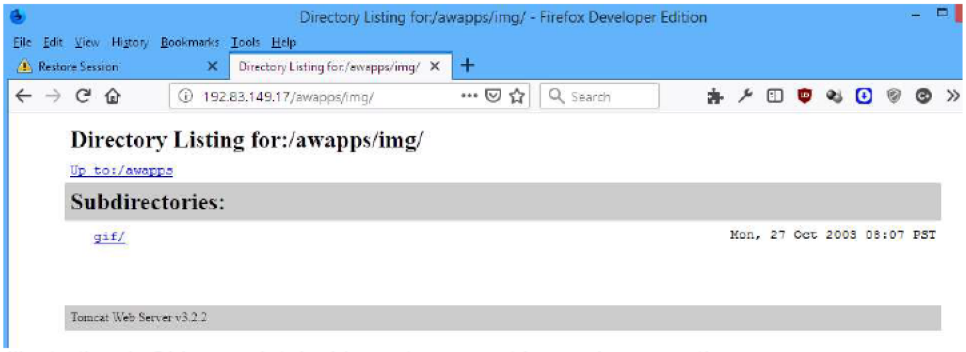
The test findings showed the CSL network to be in [redacted]. The rav is a measurement of the balance between operations, vulnerabilities, and controls. It is used to measure your security posture where 100rav is perfect balance.

Score:

Actual Security: [redacted]　　Attack Surface: [redacted]

For usability, that score is translated into a percentage for the attack surface, the area left uncontrolled or vulnerable, which is the difference between 100rav and the rav score. An attack surface greater than 10% is considered problematic as it is “reactive security” and will require heavy resources to maintain security. An attack surface greater than 20% is considered difficult and likely to be already breached.

Security Assessment


Directory Listing for:/awapps/img/ - Firefox Developer Edition
File Edit View History Bookmarks Tools Help
Restore Session
Directory Listing for:/awapps/img/
192.83.149.17/awapps/img/
Search

Directory Listing for:/awapps/img/

Up to:/awapps

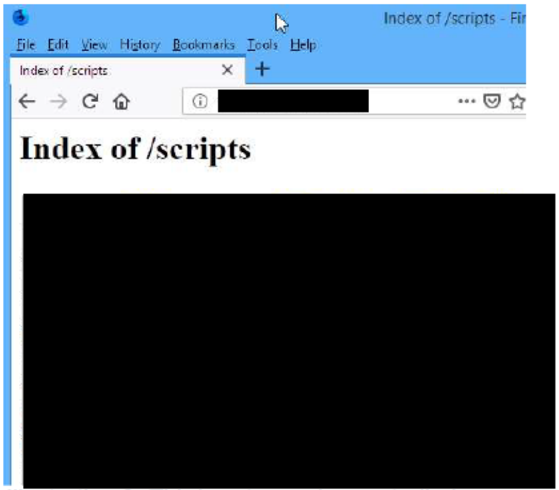
Subdirectories:

gif/ Mon, 27 Oct 2003 08:07 PST

Tomcat Web Server v3.2.2

Illustration 1: Old, unmaintainable systems must be run in quarantine.

The CSL network appears complicated at first look however it’s a [redacted] This shows an inherent vulnerability in the infrastructure that [redacted] This also assures Single Points of Failure where a Denial of Service Attack on any of a majority of the systems will lead to all systems being unusable. The first step to security is [redacted] which CSL has no control over and [redacted]



[redacted]

Index of /scripts

[redacted]

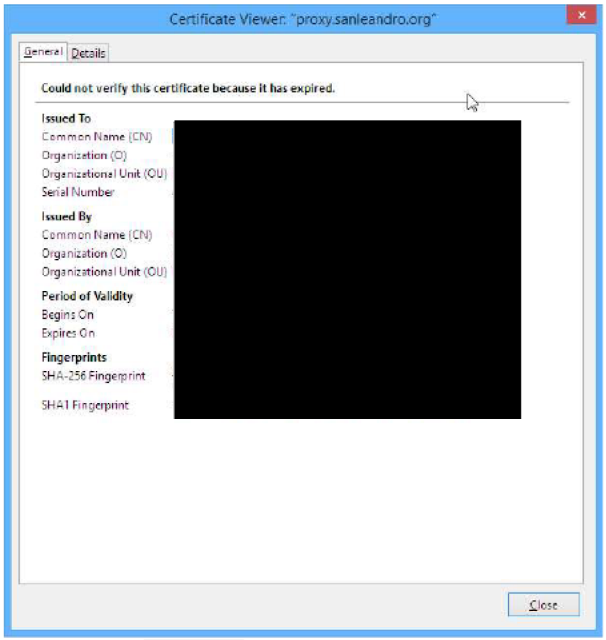
Illustration 2: Third-party vendor-controlled systems must be separated from CSL systems.

The next noteworthy issue [redacted]

[redacted]

[redacted]

[redacted]



Certificate Viewer: "proxy.sanleandro.org"

Could not verify this certificate because it has expired.

Issued To
Common Name (CN)
Organization (O)
Organizational Unit (OU)
Serial Number

Issued By
Common Name (CN)
Organization (O)
Organizational Unit (OU)

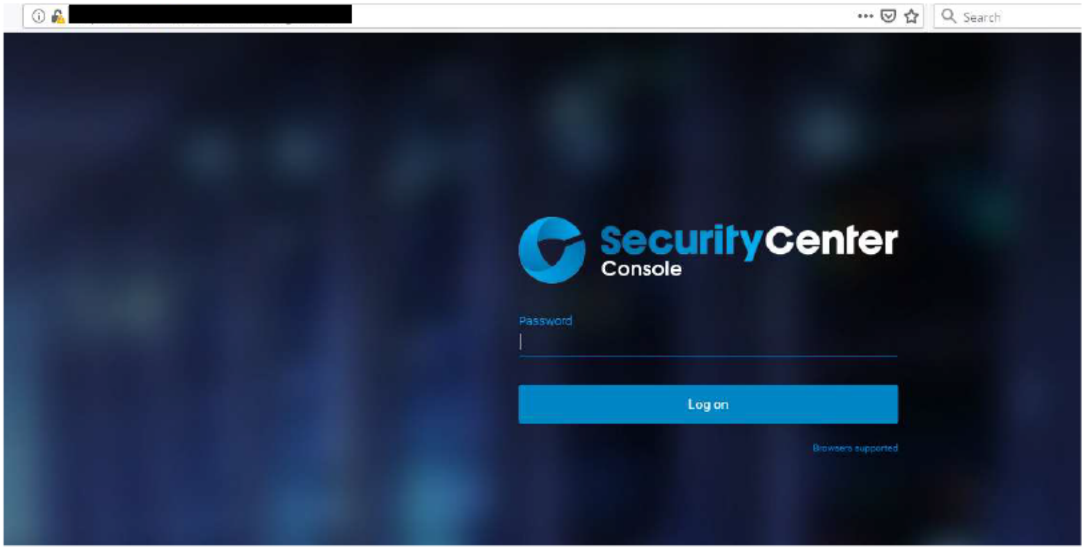
Period of Validity
Begins On
Expires On

Fingerprints
SHA-256 Fingerprint
SHA1 Fingerprint

[redacted]

Illustration 3: [redacted] *server certificates and cryptography protocols.*

[redacted]



[redacted]

Illustration 4: Security device administration is exposed.

[redacted]

[redacted]

Remediation

As a company which provides a cryptographically secure and resilient means for protecting your critical network data, keys, and assets, we have identified many places where CryptoMove can integrate its products within the CSL network which would greatly improve security, integrity, and privacy. However, this alone will not protect availability of the data if CSL does not address critical concerns.

It is our recommendation that remediation start as the following in this order:

1. Lock down critical assets with CryptoMove.

At this point you've closed off vulnerable servers and services however without a forensic investigation, you can't know if you've already been compromised. Therefore it's important to lock down critical assets, keys, and personal data as quickly as possible. This is actually the fastest way for you do that without a large team of IT personnel cleaning or reinstalling all your systems.

2. Segment the network to separate systems,

putting Vendor and 3rd party systems together, quarantining older operating systems which can't be maintained into smaller sandboxes that are not directly connected to the Internet or other systems, and critical and administration systems from the rest. Separate authentication credentials by changing current and default login accounts and resetting all user passwords in case of compromise.

3. Separate administrative access to machines

through a bastion host so no direct access for login is available over the Internet. This provides a form of 2-factor authentication which makes the system substantially more secure.

4. Harden the systems to least privilege,

remove defaults in passwords and users, close unused services, remove remote development services, and update operational controls like cryptographic methods and certificates. Remove unneeded applications and server-side technologies from web servers.

5. Get a monitoring system in place,

preferably one with automation and intrusion response. This can be a SIEM or an IDS/IPS. The most important rules you’ll require initially are controlling how much data can move from one system over a given time period, how many attempts one can make to any login, and non-repudiation over what systems and users are accessing at any given time.

6. Address your information leaks,

especially the DNS inconsistencies. Visibility research lead to the following systems which make up the engagement zone, considered “opportunity” in the attack surface and the interactive parts of the scope. Therefore review these domains and addresses with your records to assure that your information is correct as this is how your configurations reveal your environment to the Internet:

```
No IP associated with [redacted]

[redacted]           ftp.sanleandro.org
[redacted]           ts.sanleandro.org
[redacted]
[redacted]           smtp-02-b.ci.san-leandro.ca.us
[redacted]           ns1.sanleandro.org
[redacted]           ns2.ci.san-leandro.ca.us, ns3.ci.san-leandro.ca.us,
            ns3.sanleandro.org
[redacted]           weblink.sanleandro.org
[redacted]           mpx1.ci.san-leandro.ca.us
[redacted]           legacy.sanleandro.org
[redacted]           archive.sanleandro.org
[redacted]           proxy.sanleandro.org
[redacted]           ch-webext.sanleandro.org
[redacted]           ise.sanleandro.org
[redacted]           ch-adfs1.sanleandro.org
[redacted]           pd-adfs1.sanleandro.org
[redacted]
[redacted]           paysllibrary.sanleandro.org
[redacted]           access.sanleandro.org
[redacted]
[redacted]           ch-sbc1.sanleandro.org
```

[redacted] ch-sbc2.sanleandro.org

Exceptions

The following system is hosted yet vital to the scope therefore it was tested carefully without the use of exploits:

[redacted] sanleandro.org, www.sanleandro.org,
www.sanleandropubliclibrary.com,
www.sanleandropubliclibrary.org, www.sanleandrolibrary.com,
www.sanleandrolibrary.org

Extended Scope

The following systems were not within the engagement zone because they resided with third parties therefore they were not tested however your infrastructure is tied to these systems.

[redacted] san-leandro.ca.us, www.san-leandro.ca.us,
sanleandro.onmicrosoft.com, autodiscover.outlook.com,
autodiscover.sanleandro.org, login.microsoftonline.com

[redacted] sip.sanleandro.org
sanleandrolibrary.org, rs-webhost-03.pixelpushers.com

[redacted] energytracker.sanleandro.org

[redacted] h*.ds3atm-ch.ci.san-leandro.ca.us

7. Address your system vulnerabilities.

The weaknesses and vulnerabilities in your systems are [redacted] However most can be fixed by simply fully updating your systems to current versions. However, the previous steps you've taken towards securing your network have already addressed many of the dangers that these vulnerabilities could have caused. Here is a list of the systems with most critical vulnerabilities:

[redacted]

According to its self-reported version number, the installation of Microsoft Internet Information Services (IIS) 6.0 on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

[redacted]

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. [redacted]. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.
For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, [redacted] Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

[redacted]

The remote host supports [redacted] and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a [redacted] and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection [redacted]
It is possible to query the remote name server for third-party names. [redacted] then it allows anyone to use it to resolve third party names. This allows attackers to perform cache poisoning attacks against this nameserver. If the host allows these recursive queries via UDP, [redacted]

[redacted]

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do. The following directories are browsable:

[redacted]

Summary

The following matrix represents your current attack surface to help you see missing or unsatisfactory controls for various types of attacks. Since a matrix requires white box testing with full cooperation from staff, this matrix is limited by the test vector and therefore likely incomplete. Regardless, this matrix represents protections covering all possible types of attacks. Full coverage of all controls means you are fully protected against any kind of attack. A red X shows there is no control of this type for your infrastructure.

Control	Interactive Points			
	PHYSICAL	NETWORK	SERVER	APPLICATIONS
Authentication	[redacted]	[redacted]	[redacted]	[redacted]
Indemnification	[redacted]	[redacted]	[redacted]	[redacted]
Resilience	[redacted]	[redacted]	[redacted]	[redacted]
Subjugation	[redacted]	[redacted]	[redacted]	[redacted]
Continuity	[redacted]	[redacted]	[redacted]	[redacted]
Non-Repudiation	[redacted]	[redacted]	[redacted]	[redacted]
Confidentiality	[redacted]	[redacted]	[redacted]	[redacted]
Privacy	[redacted]	[redacted]	[redacted]	[redacted]
Integrity	[redacted]	[redacted]	[redacted]	[redacted]
Alarm	[redacted]	[redacted]	[redacted]	[redacted]

As you can see, the CSL infrastructure needs much more work beyond these recommendations. Based on your processes, it is highly recommended you build a more resilient security posture that requires much less maintenance than you have now. That will let you focus on improving technology without getting mired in putting out fires all the time like malware, breaches, and stolen user accounts.